Assessment Submission Cover Sheet

This Assessment Cover Sheet **must** be included on all Assessment submissions.

|  |  |
| --- | --- |
| Assignment Title | Assignment B – Portfolio Assessment |
| Module | Data Mining |
| Student Name  (same as Student Card) | Ciaran Finnegan |
| Student Number |  |
| Programme |  |
| Part-Time/Full-Time |  |
| Year of Study  (First Year, Second Year, etc) |  |

Late Submissions: Assessment submitted after the deadline will have a late penalty applied.

**Academic Integrity for assessment in TU Dublin Programmes**

Each student is responsible for knowing and abiding by TU Dublin Academic Regulations and Policies. Any student in breach of these regulation/policies will be subject to action in accordance with the University’s procedures for breaches of assessment regulations. Please refer to the General Assessment Regulations at

<https://tudublin.libguides.com/c.php?g=674049&p=4794713>

<https://www.tudublinsu.ie/advice/exams/breachesofregulations/>

All students are expected to complete their courses/programmes in compliance with University regulations. No student shall engage in any activity that involves attempting to receive a grade by means other than honest effort, for example:

1. No student shall complete, in part or in total, any examination or assessment for another person.
2. No student shall knowingly allow any examination or assessment to be completed, in part or in total, for themselves by another person.
3. No student shall plagiarise or copy the work of another and submit it as their own work.
4. No student shall falsify any data. Falsification is the invention of data, its alteration, its copying from any other source, or otherwise obtaining it by unfair means, or inventing quotations and/or references.
5. No student shall use aids or devices excluded by the lecturer in undertaking course work or assessments/ examinations.
6. No student shall knowingly procure, provide, or accept any materials that contain questions or answers to any examination or assessment to be given at a subsequent time.
7. No student shall provide their assignments, in part or in total, to any other student in current or future classes of this module/ programme unless authorised to do so by the lecturer.
8. No student shall submit substantially the same material in more than one module/programme without prior authorization.
9. No student shall alter graded assignments or examinations and then resubmit them for regrading, unless specifically authorised to do so by the lecturer.
10. All programming code and documentation, unless correctly referenced, submitted for assessment or existing in the student’s computer accounts must be the students’ original work or material specifically authorized by the lecturer.
11. Collaborating with other students to develop, complete or correct course work is limited to activities explicitly authorized by the lecturer.
12. For all group assignments, each member of the group is responsible for the academic integrity of the entire submission. Consequently, all group members must satisfy themselves that all elements of their submission adhere to the academic integrity statement points above.

By submitting coursework, either physically or electronically, you are confirming that it is your own work (or, in the case of a group submission, that it is the result of joint work undertaken by members of the group that you represent) and that you have read and understand the University’s Regulations and Policies covering Academic Integrity (see General Assessment Regulations)*.*

Coursework may be submitted to an electronic detection system in order to help ascertain if any plagiarised material is present. If you have queries about what constitutes plagiarism, please speak to your lecturer.

|  |  |
| --- | --- |
| Student Signature |  |
| Date |  |

IMPORTANT:

* Complete the required number of tasks as defined in Assessment Handout
* The sections listed below are an example of the section headings for each task. You can use alternative headings
* Tasks 1-3: Sub-Sections 1-7 should be no longer than 8 pages (minimum 6 pages), including diagrams, images, screen captures, tables, etc. Careful selection of these is needed.
  + Code does not count to this total. Code should be added to the relevant section.
* Detailed discussion is expected. Marks are awarded based on depth of information given.
* Marks are awarded based on complexity of problem and depth of work.

# TASK 4 – *Ethics and the user of Data Science/ML/AI*

## Task 4-1 : Stop The Killer Robots – Autonomous Drone Warfare

1. **Overview of problem**
2. **Ethical and Legal Challenges**

The MoD says its policy is that only humans will be able to fire weapons, although there is growing concern about the potential danger of unrestricted robot warfare, led by the Campaign to Stop Killer Robots.

Technology under development includes the i9 drone, which is powered by six rotors and carries two shotguns. Remotely operated, it is intended to be used to storm buildings, typically an urban warfare situation that generates some of the highest casualties.

the Pentagon faces the daunting challenge of working through a plethora of ethical issues surrounding the technology while staying ahead of advanced adversaries who are pursuing their own capabilities.

An effective ‘AI Arms Race’.

In August, heads were turned when an AI agent defeated a seasoned F-16 fighter pilot in a series of simulated combat engagements during the final round of the Defense Advanced Research Projects Agency’s “Alpha Dogfight” Trials. The agent, developed by Heron Systems, went undefeated with a record of 5-0 against the airman whose call sign was “Banger.”

“It’s a significant moment,” said Peter W. Singer, a strategist and senior fellow at the New America think tank, comparing it to chess master Garry Kasparov losing to IBM’s Deep Blue computer at the complex game.

During the simulated dogfight “the AI shifted [its tactics] and it kept grinding away in different ways at him” until it won, noted Singer, co-author of *Ghost Fleet* and *Burn-In*, which examine the military and societal implications of autonomy and artificial intelligence.

“That means that we have two kinds of legal and ethical questions that we’ve really never wrestled with before. The first is machine permissibility. What is the tool allowed to do on its own? The second is machine accountability. Who takes responsibility … for what the tool does on its own?”

In February, the Defense Department rolled out a list of five AI ethical principles based on recommendations from the Defense Innovation Board and other experts inside and outside of the government.

Military personnel must be responsible and exercise appropriate levels of judgment and care while remaining responsible for the development, deployment and use of AI capabilities, according to the list.

The technology should be “equitable” and steps taken to minimize unintended bias.

It must be traceable: “The department’s AI capabilities will be developed and deployed such that relevant personnel possess an appropriate understanding of the technology, development processes and operational methods applicable to AI capabilities, including with transparent and auditable methodologies, data sources, and design procedure and documentation,” according to the list.

Systems must also be reliable: “The department’s AI capabilities will have explicit, well-defined uses, and the safety, security and effectiveness of such capabilities will be subject to testing and assurance within those defined uses across their entire lifecycles.”

And finally, they must be governable: “The department will design and engineer AI capabilities to fulfill their intended functions while possessing the ability to detect and avoid unintended consequences, and the ability to disengage or deactivate deployed systems that demonstrate unintended behavior.”

1. **Challenges for Data Scientist**

The principles need to be kept in mind throughout the acquisition process and product lifecycle when officials are thinking about how to design, develop, deploy and use AI, she said.

“We’re currently working with RDT&E folks in terms of thinking through how we can integrate the ethics aspects in their test harness” for software and other technology, Patel said. “We’re looking at the testing aspects, the algorithmic aspects, the system integration, and then the human-machine teaming aspects. … All of those pieces are critical aspects or potential areas for us to embed and engage in from a responsible AI perspective.”

Artificial intelligence must work as intended, or else bad things could happen and users won’t trust it. One issue that could undermine trust is known as algorithmic bias.

“Algorithmic bias is basically when either [the system] was trained in the wrong way for a scenario that it was applied to, or it was provided biased data of some kind,” Singer explained.

For example, in the civilian world there was a case where an artificial intelligence tool was used to aid in the treatment of heart disease, but it was providing bad medical advice for African Americans. “No one told that AI, ‘You be racist,’” Singer said. “But it was, because of the way it was trained in the data.”

Scharre noted that AI is also vulnerable to hacking or spoofing attacks that could corrupt data or cause other problems.

The Pentagon will have to continually make decisions about which tasks to delegate to machines, he noted. A key question will be where humans will be in the decision-making loop.

Patel noted that implementation policies will need to ensure that the technology has disengagement mechanisms in place in case something goes wrong.

“In many cases when we think about implementation of those principles themselves, they really speak to good engineering practices in terms of capability, in terms of reliability, in terms of governability,” she said.

Experts say the world won’t be overrun by godless killing machines anytime soon. There are more pressing concerns, such as working through shortcomings in artificial intelligence and machine learning, and figuring out how best to conduct human-machine teaming.

1. **Reflections**

Singer said the Pentagon might someday loosen the restrictions it has placed on using artificial intelligence. An historical analogy is the U.S. Navy’s embrace of unrestricted submarine warfare in World War II. Moral opposition to the German use of the tactic against civilian vessels was a catalyst for the U.S. entry into World War I, he noted. But just a few hours after the Pearl Harbor attack in 1941, the order went out to wage unrestricted submarine warfare against Japan.

1. **References**

Use one of the commonly used References and Citation formats.

[The-evolution-of-disruptive-technologies-and.pdf (stopkillerrobots.org)](https://www.stopkillerrobots.org/wp-content/uploads/2021/09/The-evolution-of-disruptive-technologies-and.pdf)

[Stop Killer Robots](https://www.stopkillerrobots.org/)

## Task 4-1 : <Title of Case Study)

1. **Overview of problem**
2. **Ethical and Legal Challenges**
3. **Challenges for Data Scientist**
4. **Reflections**
5. **References**

Use one of the commonly used References and Citation formats.